UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,552	08/16/2006	Giovanni Ghigo	09952.0069	8465

22852 7590 03/04/2009

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/589,552	**Applicant(s)** GHIGO ET AL.	
	Examiner BRYAN WRIGHT	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/.20/2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19-36* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to Amendment filed 12/02/2008.

2. Claims 19-36 are pending.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 19 recites the limitation "said generator" in line 15. There is insufficient antecedent basis for this limitation in the claim. Applicant recites in a pseudo-random number generator and a true random number generator. The basis for the statement of "said generator" cannot be differentiated.

4. Claim 20 recites the limitation "said generator" in line 2. There is insufficient antecedent basis for this limitation in the claim. Applicant recites in a pseudo-random number generator and a true random number generator. The basis for the statement of "said generator" cannot be differentiated.

5. Claim 26 recites the limitation "said generator" in lines. There is insufficient antecedent basis for this limitation in the claim. Applicant recites in a pseudo-random number generator and a true random number generator. The basis for the statement of "said generator" cannot be differentiated.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

6. Claims 19-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Carlson et al. (US Patent Publication No. 2005/0055391) in view of Crouch et al. (US Patent No. 5,383,143 and Crouch hereinafter).

7. As to claim 19, Carlson teaches a random number generator, comprising:

a true random number generator (i.e., … teaches a entropy generator [par. 15]);

a pseudo-random number generator arranged to generate a pseudo- random sequence by using the true random numbers produced by said true random number generator as random seed (i.e., ... teaches a Left Shift Register (e.g., pseudo-random number generator) receiving the output (e.g., seed) of the entropy generator [fig. 5]);

and a mixing logic (e.g., mixing function) connected between said true random number generator and said pseudo-random number generator and arranged to alter the behavior of said pseudo-random number generator by using the random seed (i.e., … teaches the seed from entropy generator as input to a mixing function to generate a random number [par. 15]), said true random generator being arranged to generate a random sequence of bits having variable rate (i.e., ... teaches the use of a entropy generator [par. 15]. Those skilled in the art would recognize a entropy generator use a non-deterministic source to produce truly random output), said generator of the alteration signal being connected so as to receive said seed and generate said alteration signal by processing said seed by means of the sequence generated by said pseudo- random number generator (i.e., … teaching a mixing function receiving from a entropy generator a seed [par. 15]. ... teaches a mixing function used to alter the characteristic of its input [par. 33 & 34]).

Carlson does not expressly teach the claim limitation element of a pseudo-random generator. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses: the use of a pseudo-random number generator (to provide the capability to create a random number using a pseudo-random generator [col. 8, lines 50-55];

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of producing a random number using a pseudo-random number generator as disclosed above by Crouch, for which random number generation will be enhanced [col. 8, lines 50-55].

8. As to claim 20, the system disclosed by Carlson shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

9. As to claim 20, Carlson teaches a random number generator where said generator of the alteration signal (e.g., jittery) comprises [fig. 5]:

Carlson does not expressly teach the claim limitation element of a first down counter arranged to count down from a first random number represented by a first group of bits which are part of a randomly rotated version of a seed received by said alteration signal generator, said first counter loading said first random number and starting its countdown whenever a seed is available and, between the occurrence of two subsequent seeds, whenever it generates a terminal count signal, said terminal count signal being fed to said pseudo-random number generator as alteration signal;

a second down counter which is arranged to count down from a second random number represented by a group of bits of the sequence generated by said pseudo-random number generator and is arranged to load a new value of said second random number and to start again its countdown whenever said first down counter generates its terminal count signal;

and a recirculating shift register which receives the seeds and feeds said first down counter with said first random number, and which is arranged to generate said randomly rotated version of the seed in the intervals between the arrivals of two subsequent seeds by rotating the bits of the seed by an amount determined by the value of said second random number.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses:

a first down counter arranged to count down from a first random number represented by a first group of bits which are part of a randomly rotated version of a seed received by said alteration signal generator (to provide a N-bit counter means to count the length of the vector (e.g., bit sequence) output from a LFSR (e.g. alteration signal generator) [col. 7, lines 15-20]), said first counter loading said first random number and starting its countdown whenever a seed is available and (to provide the loading of a bit sequence (e.g., first random number) upon changing of the seed [col. 11, lines 15-35]), between the occurrence of two subsequent seeds whenever it generates a terminal count signal said terminal count signal being fed to said pseudo-random number generator as alteration signal (to provide input into a LFSER (e.g., pseudo-random generator) as a alteration signal [col. 6, lines 3-6]);

a second down counter which is arranged to count down from a second random number represented by a group of bits of the sequence generated by said pseudo-random number generator and is arranged to load a new value of said second random number and to start again its countdown whenever said first down counter generates its terminal count signal (to provide a second N-bit counter arranged to count the number of bit sequence (e.g., second random number) and control cycling through seed values based on activated control logic (e.g., terminal count signal) [col. 2, lines 50-67]);

and a recirculating shift register (e.g., LFSR) which receives the seeds and feeds said first down counter (e.g., second register) with said first random number (to provide a second register for receiving a random number based on installed seed value [col. 5, lines 20-30]), and which is arranged to generate said randomly rotated version of the seed in the intervals between the arrivals of two subsequent seeds by rotating the bits of the seed by an amount determined by the value of said second random number (to provide means to generate seed variation using bit rotation based on generated random numbers [col. 6, lines 45-60]).

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of producing a random number using a pseudo-random number generator as disclosed above by Crouch, for which random number generation will be enhanced [col. 8, lines 50-55].

10. As to claim 21, Carlson teaches a random number generator where said pseudo-random generator is a linear feedback shift register and said alteration signal generator supplies said alteration signal to the feedback logic of said linear feedback shift register [col. 5, lines 5-10].

Carlson does not expressly teach the claim limitation element of a pseudo-random generator. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses: the use of a pseudo-random number generator (to provide the capability to create a random number using a pseudo-random generator [col. 8, lines 50-55];

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of producing a random number using a pseudo-random number generator as disclosed above by Crouch, for which random number generation will be enhanced [col. 8, lines 50-55].

11. As to claim 22, Carlson teaches a random number generator where said mixing logic (e.g., mixing function) further comprises an input circuitry arranged to receive the random sequence of bits generated by said true random generator (e.g., entropy generator) to build said seed by parallelising (e.g., duplicating [par. 34]) the bits of said random sequence and to generate a signal indicating the availability of a seed [par. 15].

Carlson does not expressly teach the claim limitation element of generating a signal indicating the availability of a seed. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses: generating a signal indicating the availability of a seed (to provide various control signals for purpose to re-seed [col. 11, lines 15-20];

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of control signal to indicate re-seeding as disclosed above by Crouch, for which random number generation will be enhanced [col. 11, lines 15-20].

12. As to claim 23, the system disclosed by Carlson shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

A random number generator where said recirculating shift register is arranged to load a seed directly whenever it receives said signal indicating the availability of the seed, and said pseudo-random generator is arranged to load a new seed upon command of said first counter whenever the latter receives said signal indicating the availability of the seed.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses:

A random number generator where said recirculating shift register (e.g., re-seeding register) is arranged to load a seed directly whenever it receives said signal indicating the availability of the seed (to provide a re-seeding register for loading a new seed upon receiving control signal [col. 13, lines 10-15]), and said pseudo-random generator is arranged to load a new seed upon command of said first counter whenever the latter receives said signal indicating the availability of the seed (to provide a LFSR (e.g., pseudo random number generator) loading capability upon receiving appropriate control signal [col. 11, lines 15-20].

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of seed loading using a control signal as disclosed above by Crouch, for which random number generation will be enhanced [col. 13, lines 10-15].

13. As to claim 24, Carlson teaches random number generator where said input circuitry comprises a clock signal generator for generating, starting from a first clock signal timing the operations of said input circuitry, and a second clock signal for timing said pseudo-random generator and said alteration signal generator whereby the output bit rate of the random number generator is independent of the rate of the random sequence of bits supplied by the true random generator (i.e., the teaching of Carlson provides the use of a entropy generator (e.g., true random generator) and use of a control clock signal [par. 15 & 23]).

Carlson does not expressly teach the claim limitation elements of a first clock signal timing and second clock signal time to produce a variable output rate for seed generation. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses: a first clock signal timing and second clock signal time to produce a variable output rate for seed generation (to provide a multi-clock timing architecture for purpose of variable seed generation [fig. 4 & 6]);

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of a multi-clock circuit architecture for producing seed at various increments as disclosed above by Crouch, for which random number generation will be enhanced [fig. 6].

14. As to claim 25, Carlson teaches a random number generator further comprising an output logic for parallelising (e.g., duplicating) the altered pseudo-random sequence and building words of a given length (e.g., segments) [par. 34], said output logic comprising a scrambler for scrambling (e.g., duplication, concatenation, and bit paddling) the bits in each word in random manner (i.e., ... teaches the use of duplication, concatenation, and bit paddling to produce a new word [par. 34]).

15. As to claim 26, Carlson teaches a random number generator where said scrambler is controlled by a random selection signal (e.g., entropy generator output) provided by said generator (e.g., entropy generator) of the alteration signal (i.e., … Carlson teaches scrambling by duplication, concatenation, and bit paddling of the output signal [par. 34]).

16. As to claim 27, the system disclosed by Carlson shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

A random number generator where a random selection signal is supplied by said recirculating shift register.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses:

A random number generator where a random selection signal (e.g., additional) is supplied by said recirculating shift register (to provide additional seeds by means of a re-seed register [col. 13, lines 25-35]).

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of re-seeding circuitry disclosed above by Crouch, for which random number generation will be enhanced [col. 13, lines 25-35].

17. As to claim 28, Carlson reaches a random number generator where said scrambler circuit comprises a switching matrix comprised of an n-level binary tree of switches (i.e., … Carlson teaches scrambling by duplication, concatenation, and bit padding of the output signal [par. 34]), each controlled by a respective bit of said random selection signal so as to scramble or to let through unchanged its input bits (par. 16).

18. As to claim 29, Carlson teaches a random number generator (e.g., LFSR) implemented as an integrated circuit [par. 20].

19. As to claim 30, Carlson teaches a method of generation of random numbers, in which said random numbers are generated by altering (e.g., duplication, concatenation, and bit padding) a pseudo-random sequence by means of true random numbers

forming random seeds for the generation of said pseudo-random sequence [par. 34], the method comprising the steps of: obtaining the random seeds from a random sequence of bits having variable rate (i.e., … teaches a entropy generator is use to generation a random seed for which is receive into a mixing function containing LFSR [par. 15];

Carlson does not expressly teach processing a random seed to generate an alteration signal exploiting the random arrival time of the bits of said sequence of bits; and changing the pseudo-random sequence by said alteration signal at random instants between the arrival of two subsequent seeds, thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds, said alteration signal being generated under the control of the pseudo-random sequence.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses:

processing a random seed to generate an alteration signal exploiting the random arrival time of the bits of said sequence of bits (to provide the of a random seed based on bit sequencing [col. 6, lines 36-53]);

and changing the pseudo-random sequence by said alteration signal at random instants between the arrival of two subsequent seeds (to provide the capability to change a pseudo-random sequence between subsequent seed arrivals [col. 5, lines 60-67; col. 6, lines 1-10]), thereby obtaining in said interval multiple pseudo-random sequences of random lengths shorter than the lengths determined by the arrival of two subsequent seeds (to provide the capability to change seed values within a predetermined clock cycle [col. 6, lines 1-20]), said alteration signal (e.g., sequence pick) being generated under the control of the pseudo-random sequence (to provide control based on a pseudo-random sequence [the capability for seed creation using the control of a pseudo-random sequence [col. 6, lines 15-20]).

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of seed processing using a pseudo-random bit sequence as disclosed above by Crouch, for which random number generation will be enhanced [col. 6, lines 35-53].

20. As to claim 31, the system disclosed by Carlson shows substantial features of the claimed invention (discussed in the paragraphs above), it fails to disclose:

A method where said alteration signal is generated at the end of a first countdown starting from a first random number represented by a randomly variable group of bits that are part of a rotated version of a received seed obtained by rotating the seed by an amount indicated by a second random number represented by a group of bits of the pseudo-random sequence, the first countdown starting whenever a seed is generated and restarting, between the arrival of two subsequent bits, whenever the countdown itself ends;

and wherein said second random number is the starting value of a second countdown starting whenever the first down counting ends, the end of said second countdown stopping said seed rotation.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses:

A method where said alteration signal is generated at the end of a first countdown starting from a first random number represented by a randomly variable group of bits that are part of a rotated version of a received seed obtained by rotating the seed by an amount indicated by a second random number represented by a group of bits of the pseudo-random sequence (to provide seed creation utilizing a previous seed value [col. 5, lines 20-25]), the first countdown starting whenever a seed is generated and restarting, between the arrival of two subsequent bits, whenever the countdown itself ends (to provide control circuitry operating with a define clock cycle to choose another seed value based on a previous seed within a pseudo-random sequence [col. 5, lines 45-67] ;

and wherein said second random number is the starting value of a second countdown starting whenever the first down counting ends, the end of said second countdown stopping said seed rotation (to provide seed rotation capability based on a pseudo -random sequence [col. 5, lines 50-60]).

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of seed rotation using a pseudo-random bit sequence as disclosed above by Crouch, for which random number generation will be enhanced [col. 5, lines 50-60].

21. As to claim 32, Carlson teaches a method where said pseudo-random sequence is generated by a linear feedback shift register and said alteration signal is fed to the feedback logic of said linear feedback shift register [col. 5, lines 5-10].

22. As to claim 33, Carlson teaches a method where the altered pseudo- random sequence is parallelised (e.g., duplicating) to create words of a desired length and further comprising a random scrambling of said words [par. 34].

23. As to claim 34, Carlson teaches a method where said scrambling (e.g., duplication, concatenation, and bit paddling) is controlled by a random selection signal obtained from the bits used to form said first random number [par. 34].

24. As to claim 35, Carlson teaches a method further comprising the step of generating, the parallelization (e.g., duplicating) of the output words and the scrambling (i.e., … Carlson teaches the element of signal alteration through duplicating, concatenating, and bit padding [par. 34]), whereby an output bit rate independent from the rate of the random sequence of bits is obtained [par. 23].

Carlson does not teach the claim limitation element of starting from a first clock signal timing the seed generation and a second clock signal for timing the generation of said pseudo-random sequence and of said alteration signal. However, these features are well known in the art and would have been an obvious modification of the system disclosed by Carlson as introduced by Crouch. Crouch discloses: starting from a first clock signal timing the seed generation and a second clock signal for timing the generation of said pseudo-random sequence and of said alteration signal (to provide a clock signal timing for generation of a pseudo-random sequence [col. 5, lines 45-65]).

Therefore, given the teachings of Crouch, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Carlson by employing the well known feature of pseudo-random sequence generation using clock cycles as disclosed above by Crouch, for which random number generation will be enhanced [col. 5, lines 45-65].

25. As to claim 36, Carlson teaches a computer program product loadable in the memory of at least one computer and including software code portions capable of performing the method of claim 30 [par. 33].

Response to Arguments

Applicant's arguments, see Applicant's Remarks, filed 12/05/2008, with respect to the rejection(s) of claim(s) 19-36 have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Carlson and Crouch.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435